ECFS - E-mail Filing

<PROCEEDING>	Docket No. 10-255 , Framework for Next Generation 911 Deployment
<DATE>	10 Jan 2011
<NAME>	Rex Buddenberg
<ADDRESS1>	2151 Trapani Circle
<ADDRESS2>	
<CITY>	Monterey
<STATE>	Ca
<ZIP>	93940
<LAW-FIRM>	
<ATTORNEY>	
<FILE-NUMBER>	
<DOCUMENT-TYPE>	COmment
<PHONE-NUMBER>	831/646-9876
<DESCRIPTION>	Comment
<CONTACT-EMAIL>	buddenr21@comcast.net

From : Rex Buddenberg

To: Federal Communications Commission

Reference: PS Docket No. 10-255 , Framework for Next Generation 911 Deployment

Point of view. I am writing this as a private citizen.

The Next Generation 911 implementation will be a set of applications that run over an internet infrastructure [7[1]]. This understanding must be fully accommodated in an NG911 system requirements and design. Many of your own NOI citations point out that this will happen and that it's a good idea, so I'll not repeat that.

The NOI analysis of the differences between circuit-switch 911 and packet-switched 911 is incomplete. Symptoms are recognized:

> 23. Unlike communications systems that interconnect with the PSTN, IP-based communication systems are media-neutral, i.e., they can transport any digital information, regardless of content ..

This is the good news. But:

> 16. Interconnected VoIP E911. ... The most difficult challenge, however, is the inability of the VoIP device or service provider to determine the current geographic location of the caller.
>
> and
>
> 51. In a NG911 environment, however, end user devices are far more likely to be liberated from a particular transport network.

Comment: The fundamental modularity characteristic of the internet is a separation of application from infrastructure. The effect is that all inferential hints regarding authenticity of the call (and caller's location) that the old system derived from the closely coupled infrastructure are now absent. The PSAP operator has no clues (such as location or account administrative identity) to work with. This is an inherent fundamental characteristic of Internet Protocol: “The internet protocol treats each internet datagram as an independent entity unrelated to any other internet datagram. There are no connections or logical circuits (virtual or otherwise).” [RFC 791]. Trying to reinstate these characteristics is not possible in a packet switched network.

[1] [bracketed] references are to paragraphs in the NOI

Designing any application over an internet has two overarching issues that must be solved:

Security – provision of authenticity and confidentiality of the communications between a 911 caller and a PSAP.

Interoperability. The NG911 system cannot be a single application (e.g. SMS) but rather a set of interoperable applications. Some will be installed in 'smart phones' (either human-operated or inanimate [58]) and some will be installed at the PSAP and other emergency response nodes. The hallmark of these interoperable applications must be extensibility.

Additional observation. The Commission should note that the description of the past in Sections I and II is paralleled by the VHF/FM maritime communications system, essentially starting with the Bridge to Bridge Radiotelephone Act of 1969. The deficiencies differ only in detail and the solutions should be unified – consider a USCG communications center as a PSAP. This changes the scope to include international maritime, but it does not affect the technical issues regarding security and interoperability..

As indicated in [82], the NG911 issue will be inherently international (the internet is international); its scope should expressly include maritime.

Security.

There are several 'glancing blows' such as identity and location indefinition that your NOI mentions. The base issue of these surface comments is security. Two security attributes (authenticity and confidentiality) are germane, and authenticity: -- is the '911 caller' authentic or bogus? -- is the one to address first. If this core problem is addressed, then many of the more surface issues will find themselves in a position to be solved.

Object to be protected. In internet security discussions, the object of the security is often confused ([57] for example). We are, in a NG911 system, indifferent / agnostic to the security of the infrastructure – what is vital and central is security of the data. In ISO Reference Model terms, this is a layer 6 problem and cannot be solved with lower layer solutions. The data itself must be authenticated. This is conventionally done today by attaching a digital signature to the data.

Universality and ubiquity. There will be no cases in an NG911 system where authenticity is not a requirement.

Second security attribute: confidentiality. NOI recognizes there will be cases where confidentiality is a requirement but these will not be universal. This becomes a secondary issue when one understands that both the technology and infrastructure necessary (PKI) to solve the authenticity problem are fully applicable to the confidentiality one – the marginal costs to add confidentiality approach zero once authenticity is mastered.

Operational requirement recommendation: The FCC should 'type approve' [55] NG911 applications and the certification requirement here is that no end system (e.g. 911 caller or PSAP answerer) emits data that is not adorned with a digital signature. It is equally important that a PSAP's data be authenticated to a 911 caller as the accustomed reverse.

Recommendation. This 'type approval' providing end-to-end authentication of data needs to apply to 'vanilla VOIP' applications just as much as to non-voice '911 calls'. .

Recommendation - Infrastructure. The NOI touches on this in [57]: “public-key cryptography certificate to ensure that other NG911 entities can authenticate PSAPs ” but appears to greatly underestimate the scope. The PKI needs to include all potential '911 callers' (human and otherwise) to be effective. The scope is as broad as drivers licenses and vehicle / vessel identification numbers. The comment also suggests authentication of a PSAP; the proper object is authentication of the PSAP's data.

Personal privacy.

> 75. In light of the shared nature of NG911 architecture, we seek comment on whether privacy laws or regulations will need to be modified to adapt to the NG911 environment. ... How should we address concerns regarding private personal information that may be transmitted as part of an NG911 communication, for example, personal medical information that NG911 can provide to PSAPs and other third parties? ...

Comment. [74-75] surface some non-technical issues relative to personal privacy that are important. They relate to the Fourth Amendment.

Obtaining any '911' type of data constitutes an invasion of personal privacy. We make this compromise daily in order that the emergency services function. In the all-voice legacy 911 systems we have used procedural protections, often informal ones, to protect privacy.

In the case of NG911, we want Big Brother to be a really effective Big Brother and have accurate, authentic information on which to act. And we should design the applications to do that.

Conversely, in situations other than emergent ones, citizens should not be obliged to gratuitously transfer information such as location and personal activities to the government. Some social networking applications do this now; if you post a photograph, certain metadata such as when/where you took it also travels along and suddenly becomes publicly available. In many cases, this invasion of privacy is innocuous; in others it is certainly not.

Commercial businesses collect this kind of personal data from citizens all the time; most have an explicit data-sharing policy. An explicit, uniform data sharing policy for NG911 is necessary and that policy should be reflected in 'type approved' applications.

Interoperabiliy.

42. Given these limitations, we seek comment on how the increasing use of SMS may impact emergency communications and whether NG911 networks should be configured to support SMS emergency communications.

Comment. While no application should be proscribed from delivering '911 calls' to a PSAP, SMS presents several problems:

- the premier problem is that we're grasping for an answer without considering the criteria first. What makes SMS better or worse than, say, twitter? How would we know? Are either suitable for NG911? We need some objective criteria and the foundation criteria are security and interoperability. Most of the rest of this submission attempts to illuminate the interoperability aspect of this problem.
- Extensibility. In the history of the internet, no standard has survived that has not been extensible. For example Domain Name Service has served in the internet for a quarter century and has evolved through extensions to serve needs as they evolve.
- Trying to center up on a single application rather than the characteristics of multiple interoperable implementations is both counter to the Internet Engineering Task Force ethic and your own criteria [67]

Rather than detail shortcomings of existing applications, our efforts are better targeted at establishing considered requirements.

The first step toward NG911 interoperability is the tacit modularity embedded in the National Broadband Plan: applications are resident in end systems that are attached to an internetwork. This decouples the application from the internet, allowing both to evolve and grow independently of the other.

The second step is interoperability between two consenting end systems (e.g. 911 caller and PSAP answerer).

A dictated solution will simply be ignored by the open source community (the bulk of smart phone applications these days are open source – see Android for example). This will result in PSAPs getting data from these undisciplined applications which will be of doubtful authenticity and serendipitous-at-best interoperability.

The foundation requirement of a set of interoperable applications is a common data dictionary[2]. The common data dictionary needs to be in two tiers:

1. The first tier is 'data types'. This is essentially done in the Mulitmedia Internet Mail Extensions standards (MIME) in common use in both e-mail and web today. You have acknowledged this part of the requirement in [54]. See RFC 2045 (and several subsequent) -- there should be little reason to modify, and any required modifications should be easy extensions. RFC 5751 describes how to secure MIME data (S/MIME).
2. The second tier is more '911-specific' data types such as caller identity, timestamp, location, type of emergency, etc. An excellent example here is the

[2] Meta data, schema, data formats, data sentences ... all essentially synonyms.

data schema in the Common Alerting Protocol. CAP is built with Extensible Markup Language (XML) tools so the XML-sign and XML-crypt primitives can be used to provide authenticity and confidentiality respectively.

A third data standardization instance of prior art, closely related to MIME and CAP, that should be included, is the Simple Network Management Protocol Management Information Base. SNMP may provide a sound basis for what the NOI calls 'device initiated' [58].

The '911 caller', on emergency stimulus, initiates an SNMP 'trap'. Follow-on SNMP 'get' messages provide a PSAP the ability to derive more information from an inanimate 911 caller by querying information out of the 911 caller's agent MIB. SNMP agents and consoles do this today.

SNMP version 3 contains similar authenticity and confidentiality protections to both S/MIME and CAP – all three are based on public key technology and all three protect the data independent of infrastructure..

The SNMP MIB structure is explicitly open-ended and extensible.

Recommendation: To answer the questions in [54 and 55] there certainly must be interoperability standards, but they need to apply to the data, only secondarily to the application.

Recommendation. Examine Common Alerting Protocol to determine what, if any, extensions would be required to make it a standard schema for 911 caller – to – PSAP transactions. (CAP was designed with a public alerting concept in mind: PSAP – to – public). On completion, unless some unforeseen surprises occur, prescribe it.

Recommendation. Compliance with these interoperability (and security standards) need to be encouraged into open source applications, especially at the client (911 caller) end of the information system. A suggested means is to commission some compliant applications, release them (probably under GPL), and encourage their adaptation into easily-downloadable applications. Given the non-compliant corpus of freely downloadable applications there is no other way to compete.

Prior art.

Neither the authenticity nor the interoperability problems are new. But they are unfamiliar to the traditional 911 PSAP (as evidenced by your Section II treatment). And unfamiliar to an emergency services community that is experienced in voice-only communications. Nonetheless the same problems exist in other internet-based information systems. Sound and extensible solutions exist; we need not start from scratch.

While we need not start from scratch, unthinking uptake of existing internet applications is not acceptable – almost all are deficient in content security issues.

Much over-the-internet software distribution today implements the security features we need in an NG911 system (both open source and commercial software). Similarly, most mainstream implementations of e-mail user agents include S/MIME features. Adaptation is required; wholesale reinvention is not.

As [67-68] suggest, a business model is required and it is a quite different business model than the traditional 911 one. Virtually none of the NG911 development and operation belongs with the infrastructure providers (e.g. telcos). Rather, some of the significant partners must be found in the open source software community. One part of the NG911 business model must be erection of a Public Key Infrastructure that provides the basis for authenticity. A second part of the business model should have embedment of a '911 caller app' in every smart phone as its goal. This app needs a default configuration that meets both the interoperability and authenticity requirements.

Thank you for the opportunity to comment

/s/ Rex Buddenberg